

1 August 1977

MEMORANDUM FOR: Executive Secretary  
Security Committee  
Director of Central Intelligence

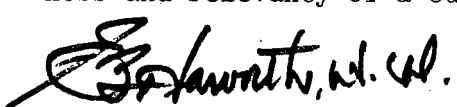
SUBJECT: Community-Wide Adherence to DCID 1/14 (U)

1. The following comments are keyed to your memorandum SECOM-D-256, 12 July 1977.
2. Para 2a. DCID 1/14 investigative standards are being followed for all individuals authorized SCI access. In cases where the initial investigation does not meet the investigative standards, the Department of the Air Force (DAF) reopens the investigation to eliminate deficiencies.
3. Para 2b. We consider the minimum standards high enough to ensure comparability of SCI screening among the Intelligence Community. Presently, a SECOM Working Group is performing a detailed analysis of those standards. The Group's review and findings should provide data to support any required revisions.
4. Para 2c. Reinvestigations of personnel indoctrinated for SCI access are conducted on a recurring 5-year basis. Pertinent special background investigation (SBI) data is maintained on SCI indoctrinated personnel by a computerized accounting system as an integral part of the Air Force SCI billet structure. Air Force directives require that appropriate actions be initiated to update the SBI 6 months prior to the 5-year expiration date.
5. Para 2d. Continuing SCI security programs are tailored to unit mission and security environment and include relevant information concerning security policy, operating procedures and practices, information regarding espionage and counterespionage efforts, and serious security incidents which occur within the intelligence community programs. DAF has implemented these programs through required semi-annual training (i.e. lectures, reading, audio-visual, etc.), a security supervisory program, and an informal newsletter. All personnel are reindoctrinated (security and operational purposes) for these programs at 2-year intervals. A reporting system has also been established for timely reporting to headquarters security managers on personal and behavior data and incidents which could affect an individual's continued access to SCI. The system also requires reporting actions of members of the immediate family of personnel when there is reason to suspect that these actions may impact upon his/her continued eligibility for SCI access. Our security supervisory program is tied closely to that reporting system. Our continuing security programs are considered to be motivating and effective. We believe, however, that the effectiveness of these programs could be improved if there were full-time professional training personnel assigned. Our special security officers and staff executive/administrative officers perform security education and training functions as an additional duty. I recommend that a centralized program be established at the national level, staffed with professional

**USAF review(s) completed.**

educators as training personnel and charged with the responsibility for developing and disseminating to members of the intelligence community, policy guidance and the high quality security education product required for this sensitive and highly important function. Suggest that the final report of the SECOM Security Awareness Working Group be evaluated prior to establishing any new policy and requirements.

6. Para 2e. Within DOD, there are no formal requirements or procedures for exchanging derogatory information used as a basis for denying SCI access. However, DOD agencies have on occasion, exchanged information, e.g. in cases where significant derogatory information appears on an individual and there are indicators that the individual was previously considered for SCI access by another agency. The need for this intra-DOD contact is minimal as the Defense Investigative Service (DIS) data made available to the former agency is also made available to us by DIS. Additionally, DIS will normally collect significant derogatory information which has evolved since the former agency's SCI access actions. One benefit which may be derived, however, is that of obtaining derogatory information which may have developed while an individual was accessed by another agency, and was used as a basis for debrief. It is conceivable that the SBI used by the previous agency for access purposes could still be current and thus would not contain the derogatory information which led to the debrief. Prior to developing such exchange procedures, perhaps we should first examine the requirement and answer questions as: Do the SBIs conducted for SCI access by the various agencies basically produce the same results and successes? What are the chances that a current SBI would not uncover significant derogatory information previously available to another agency? Will the security gain, if any, justify the additional resource demands? Will not the content, timeliness and relevancy of a current SBI suffice for SCI adjudicative purposes?

*for*   
RUSSELL T. NEWMAN, Colonel, USAF  
USAF Member